IN THE CLAIMS:

No amendments have been made to the claims

1. (Previously Presented) A Bluetooth based security system, comprising:

a secured device (SD) equipped with a Bluetooth (BT) transceiver;

a plurality of Bluetooth Access Points (BTAPs) located at designated points to establish a BT link with said secured device (SD) to receive data from and transmit data to said secured device (SD); and

a security server (SS) connected to all BTAPs and arranged to provide access control and security services for said secured device (SD),

wherein said security server (SS) to obtain attribute information of said secured device (SD), including an unique device identification (ID) and a last known location of said secured device (SD), to activate a lock with said secured device (SD), and to send location information of a designated BTAP and an unlock code to said secured device (SD), via said designated BTAP.

2. (Original) The Bluetooth based security system as claimed in claim 1, wherein said attribute information of said secured device (SD) is captured by the BTAPs and registered in a database of said security server (SS).

3. (Original) The Bluetooth based security system as claimed in claim 1, wherein said lock is activated between said secured device (SD) and said security server (SS), via said

designated BTAP, upon a request from said secured device (SD) or upon an expiration of a pre-defined timeout value of said security server (SS).

4. (Original) The Bluetooth based security system as claimed in claim 1, wherein said security server obtains the unique device identification (ID) from said secured device (SD) and the last known location of said secured device (SD) from the last BTAP that said secured device (SD) connected with.

5. (Original) The Bluetooth based security system as claimed in claim 1, wherein said security server (SS) is connected to the Internet or other networks to provide remote monitoring and tracking of said secured device (SD).

6. (Original) The Bluetooth based security system as claimed in claim 1, wherein said security server (SS) is configured to notify the owner of said secured device (SD) if said secured device (SD) is lost through unauthorized BT disconnection.

7. (Original) The Bluetooth based security system as claimed in claim 1, wherein said secured device (SD) sends the unlock code back to said security server (SS) to disengage the lock, thereby making said secured device (SD) free to roam.

8. (Original) The Bluetooth based security system as claimed in claim 1, wherein said security server (SS) comprises: a database arranged to store attribute information of said secured

device (SD), including the unique device identification (ID) and the last known location of said secured device (SD);

a processor configured with a security control software to provide ad-hoc security services, including remote monitoring and tracking of said secured device (SD); and

an I/O subsystem arranged to install the security control software and change system settings and configurations, and to establish connections with the Internet or other networks to provide security services, including remote monitoring and tracking of said secured device (SD).

9. (Original) The Bluetooth based security system as claimed in claim 8, wherein said secured device (SD) comprises:

a processor;

a host chipset connected to the processor;

a memory connected to the host chipset and arranged to contain an operating system (OS) and a security control software for activating/deactivating a lock with the BTAPs; and

a Bluetooth transceiver connected to the host chipset and arranged to contain an antenna complex for establishing communication with any of the BTAPs for security services.

10. (Original) The Bluetooth based security system as claimed in claim 9, wherein said secured device (SD) further comprises:

a Global Positioning System (GPS) receiver connected to the host chipset and arranged to contain an antenna complex for providing radio positioning and navigation needs, including

receiving location information of said secured device (SD) relative to the BTAPs and determining a change in distance between said secured device (SD) and said designated BTAP.

11. (Original) The Bluetooth based security system as claimed in claim 9, wherein said Bluetooth transceiver contains the unique device identification (ID) of said secured device (SD) for identification and communication with any one of the BTAPs strategically located at designated points where said secured device (SD) is most likely secured temporarily or permanently.

12. (Original) The Bluetooth based security system as claimed in claim 11, wherein said Bluetooth transceiver comprises:

a radio-frequency (RF) unit arranged to transmit/receive radio waves to/from any one of the BTAPs, via the antenna complex;

a baseband unit arranged to establish link set-up (control) and support for link management between said secured device (SD) and the BTAPs, including user authentication and link authorization; and

a Bluetooth data processor arranged to process sample Bluetooth data, including the location of the last BTAP that said secured device (SD) connected with.

13. (Original) The Bluetooth based security system as claimed in claim 10, wherein said GPS receiver comprises: a radio-frequency (RF) unit arranged to receive GPS data from a plurality of GPS satellites, via the antenna complex;

a baseband unit arranged to sample GPS data; and

a GPS data processor arranged to process sample GPS data relating to the location of said secured device (SD) relative to the BTAPs and determine a change in distance between said secured device (SD) and said designated BTAP.

14. (Original) The Bluetooth based security system as claimed in claim I, wherein, when said lock is activated between said security server (SS) and said secured device (SD), via said designated BTAP, said security server (SS) transmits the location information (X, Y, Z coordinates) of said designated BTAP and the unlock code to said secured device (SD) for future use, and then said secured device (SD) transmits the unique device ID of said secured device (SD) and the last know location (X, Y, Z coordinates) of said secured device (SD) back to said security server (SS), via said designated BTAP through the BT link.

15. (Original) The Bluetooth based security system as claimed in claim 14, wherein said security server (S5) creates log entry in its database, stores the unique device ID of said secured device (SD), the last known location (X, Y, Z coordinates) of said secured device, the time, and the unlock code.

16. (Original) The Bluetooth based security system as claimed in claim 15, wherein, if there is an occurrence of an unauthorized breach event during the time when the lock between said security server (SS) and said secured device (SD) is maintained, said security server (SS) operates in a search and arrest mode to notify an appropriate personnel along with the last known position of said secured device (SD) and initiate a network wide (or Internet wide) search and arrest request for said secured device (SD).

17. (Original) The Bluetooth based security system as claimed in claim 16, wherein said lock is deactivated if the user at said secured device (SD) input the unlock code, and the user supplied unlock code matches the stored unlock code.

18. (Previously Presented) A method of providing security services for a secured device equipped with Bluetooth, comprising:

installing a plurality of Bluetooth Access Points (BTAPs) at designated points to establish a BT link with said secured device (SD);

connecting a security server (SS) to all BTAPs to provide access control and security services for said secured device (SD); and

after said secured device (SD) establishes a BT link to send and receive data with a designated BTAP, enabling said security server (SS) to obtain attribute information of said secured device (SD), including an unique device identification (ID) and a last known location of said secured device (SD), activate a lock with said secured device (SD), and send location information of a designated BTAP and an unlock code to said secured device (SD), via said designated BTAP.

19. (Original) The method as claimed in claim 18, wherein said attribute information of said secured device (SD) is captured by the BTAPs and registered in a database of said security sewer (SS).

20. (Original) The method as claimed in claim 18, wherein said lock is activated between

said secured device (SD) and said security server (SS), via said designated BTAP, upon a request from said secured device (SD) or upon an expiration of a pre-defined timeout value of said security server (SS).

21. (Original) The method as claimed in claim 18, wherein said security server obtains the unique device identification (ID) from said secured device (SD) and the last known location of said secured device (SD) from the last BTAP that said secured device (SD) connected with.

22. (Original) The method as claimed in claim 18, wherein said security server (SS) is connected to the Internet or other networks to provide remote monitoring and tracking of said secured device (SD).

23. (Original) The method as claimed in claim 18, wherein said security server (SS) is configured to notify the owner of said secured device (SD) if said secured device (SD) is lost through unauthorized BT disconnection.

24. (Original) The method as claimed in claim 18, wherein said secured device (SD) sends the unlock code back to said security server (SS) to disengage the lock, thereby making said secured device (SD) free to roam.

25. (Original) The method as claimed in claim 18, wherein, when said lock is activated between said security server (SS) and said secured device (SD), via said designated BTAP, said

security server (SS) transmits the location information (X, Y, Z coordinates) of said designated BTAP and the unlock code to said secured device (SD) for future use, and then said secured device (SD) transmits the unique device ID of said secured device (SD) and the last know location (X, Y, Z coordinates) of said secured device (SD) back to said security server (SS), via said designated BTAP through the BT link.

26. (Original) The method as claimed in claim 18, wherein said security server (SS) creates log entry in its database, stores the unique device ID of said secured device (SD), the last known location (X, Y, Z coordinates) of said secured device, the time, and the unlock code.

27. (Original) The method as claimed in claim 18, wherein, if there is an occurrence of an unauthorized breach event during the time when the lock between said security server (SS) and said secured device (SD) is maintained, said security server (SS) operates in a search and arrest mode to notify an appropriate personnel along with the last known position of said secured device (SD) and initiate a network wide (or Internet wide) search and arrest request for said secured device (SD).

28. (Original) The method as claimed in claim 18, wherein said lock is deactivated if the user at said secured device (SD) input the unlock code, and the user supplied unlock code matches the stored unlock code.

29. (Previously Presented) A computer readable medium having stored thereon a plurality of instructions which, when executed by a processor of a security server (SS)

providing security services for a secured device (SD) equipped with Bluetooth via a plurality of Bluetooth Access Points (BTAPs), cause the processor to perform:

establishing a link with said secured device (SD) to receive data from and transmit data to said secured device (SD) via a designated BTAP, when said secured device (SD) is in proximity of said designated BTAP;

obtaining attribute information of said secured device (SD), including an unique device identification (ID) and a last known location of said secured device (SD);

activating a lock with said secured device (SD), via said designated BTAP, upon a request from said secured device (SD) or upon an expiration of a pre-defined timeout value;

sending location information of said designated BTAP and an unlock code to said secured device (SD), via said designated BTAP.

30. (Original) The computer readable medium as claimed in claim 29, further enabling, if there is an occurrence of an unauthorized breach event during the time when the lock between saidsecurity server (SS) and said secured device (SD) is maintained, operation in a search and arrest mode to notify an appropriate personnel along with the last known position of said secured device (SD) and initiate a network wide (or Internet wide) search and arrest request for said secured device (SD).